

# 数据跨境流动的法治挑战与应对

杜 昕

(中共广东省委党校 法学教研部, 广东 广州 510030)

**摘 要:** 数据跨境流动正在成为连接全球数字经济的纽带, 我国应积极融入并引领数字经济全球化。然而, “‘滴滴出行’赴美上市”事件却暴露出了数据跨境流动在国家安全和个人数据保护层面提出的法治挑战。我国针对挑战采取了一系列立法活动, 但是在法治实践当中仍面临两大困难, 即重要数据目录的动态管理和个人数据保护与经济协调平衡。综合当前立法与相关理论发现, 引入区块链技术, 用技术监管技术的法治思维是解决这两大实践难点的有效途径。

**关键词:** 数据跨境流动; 国家安全; 个人数据保护; 区块链技术

中图分类号: DF01

文献标识码: A

DOI: 10.19358/j.issn.2097-1788.2023.01.006

引用格式: 杜昕. 数据跨境流动的法治挑战与应对[J]. 网络安全与数据治理, 2023, 42(1): 45-53.

## Challenges and responses to cross-border data flows

Du Xin

(School of Law, Party School of Guangdong Provincial Committee of CPC, Guangzhou 510030, China)

**Abstract:** The cross-border flow of data is becoming the link connecting the global digital economy. China should actively participate in and lead the globalization of the digital economy. However, the US listing of Didi Chuxing has exposed the national security and personal data protection challenges posed by cross-border data flows. Our country has adopted a series of legislative activities in response to the challenge, but in the practice of rule of law still faces two big difficulties, namely the dynamic management of important data catalog and the balance between personal data protection and economic development. Based on the current legislation and related theories, it is found that the legal thinking of introducing block chain technology and using technology to supervise technology is an effective way to solve these two practical difficulties.

**Key words:** data flows across borders; national security; personal data protection; block chain technology

### 0 引言

习近平总书记强调:“数字经济发展速度之快、辐射范围之广、影响程度之深前所未有,正在成为重组全球要素资源、重塑全球经济结构、改变全球竞争格局的关键力量”<sup>[1]</sup>。随着数字经济的不断发展,以数据要素为核心驱动力,以网络传播技术为载体的高速率、大容量、低延时的数据跨境流动,正在成为连接全球数字经济的纽带,大大拓宽了传统经济全球化的广度与深度,数字经济全球化已经成为了历史发展的必然趋势。据此,我国应在

维护国家安全的前提下,主动拓宽数据开放范围,加快数据跨境流动,在全球竞争中进一步发挥人口优势与规模优势,积极融入并引领新一轮经济全球化。

党的二十大报告指出:“加强重点领域、新兴领域、涉外领域立法,统筹推进国内法治和涉外法治”<sup>[2]</sup>,数据跨境流动作为数字经济全球化的驱动力,是新时代相关领域的立法调整对象,数据跨境流动提出的挑战是推进涉外法治建设不能忽视的重要问题。以“‘滴滴出行’赴美上市”事件为例,根

据2022年7月21日国家互联网信息办公室(以下简称“国家网信办”)有关负责人就相关行政处罚的决定答记者问可知,滴滴公司在事件当中“存在严重影响国家安全的数据处理活动”并且“严重侵害用户个人信息权益”<sup>[3]</sup>。“‘滴滴出行’赴美上市”事件虽然以行政处罚决定<sup>[4]</sup>的作出而告终,但却暴露出一个现实问题——数据跨境流动会对国家安全和个人数据保护层面形成诸多法治挑战。如何推进我国涉外法治建设以应对数据跨境流动提出的国家安全和个人数据保护层面的法治挑战,是本文的关注点所在。

## 1 数据跨境流动提出的法治挑战

### 1.1 国家安全层面的挑战

美国达特茅斯大学塔克商学院院长、原白宫经济顾问委员会成员马修·斯劳特和桥水基金联合首席执行官大卫·麦考密克合作发表的文章《数据即力量(Data is Power)》中指出:“即便与全球经济的其他要素相比,数据与力量的关联也更为密切”<sup>[5]</sup>。国外还有学者认为“数据总是在被不断加工、分析,数据的分析解释过程蕴含着它的变革力量”<sup>[6]</sup>。我国学者也指出“拥有数据存储和处理技术优势的主体对特定对象的影响力和控制力不断增强”<sup>[7]</sup>。数据蕴含的力量如果被合法地分析利用,会极大促进经济社会的发展,保障国家的安全,例如挖掘网络媒体上人们公开发表的一些观点看法(包括对个人、话题和事件的评估、态度和情绪),通过进行数据分析,有利于防范不当言论对社会造成的负面影响,从而维护国家安全<sup>[8]</sup>。但是,大量数据一旦被不法利用,可能严重威胁国家安全,甚至导致政治动荡局面。例如,2018年曝光的“剑桥分析丑闻”<sup>[9]</sup>,8700万用户数据因Facebook出于商业决策主动对第三方程序开放宽松的API数据接口,被不当泄露给政治咨询公司剑桥分析(Cambridge Analytica),用于在2016年总统大选时支持共和党候选人特朗普。对此,国外学者评论道:“社交媒体公司和剑桥分析等政治数据挖掘公司通过使用个人数据操纵公众生活建立了自己的业务。他们的工作加剧了种族紧张关系,复兴了极端民族主义,加剧了政治冲突,甚至在世界各地的国家制造了新的政治危机——所有这些削弱了公众对新闻、投票制度和选举结果的信任”<sup>[10]</sup>。“剑桥分析丑闻”等数据不法利用的事件严重影响了政治选举的公平,加剧了美国社会

的割裂,危及了国家和政治的安全。所以,防范数据被不法利用,对于维护国家安全至关重要。

在“‘滴滴出行’赴美上市”事件当中,滴滴公司共存在16项违法事实<sup>[3]</sup>,其违法获取或过度收集的用户信息每一项的数量级均在千万以上,有些甚至过亿。直接获取的信息种类包括用户手机相册中的截图信息、用户剪切板信息和应用列表信息、乘客人脸识别信息、年龄段信息、职业信息、亲情关系信息、打车地址信息,以及乘客评价代驾服务、App后台运行、手机连接记录仪设备时的精准位置(经纬度)信息。除乘客以外,司机的身份信息、学历信息也被违法收集。这些信息被违法收集以后,滴滴在未明确告知用户的情况下,分析得出的间接信息的数量级则均以“亿”计,这些信息包括乘客的出行意图、常驻城市、异地商务或异地旅游情况,其中分析得出的乘客出行意图信息竟高达539.76亿条。

如此大规模的数据信息,一旦被不法利用,例如用以分析预测我国城市居民的出行情况和人群实时分布情况等,无疑会对我国的公共安全乃至国家安全造成严重威胁。“‘滴滴出行’赴美上市”事件起始于2021年6月30日,彼时美国《外国公司问责法》(以下简称“HFCAA法案”)<sup>[11]</sup>已经生效,该国颁布“CLOUD法案”也已届三年。“HFCAA法案”第三部分规定了向赴美上市外国企业提供服务的会计师事务所负有“额外披露”的义务,需要在审计报告中向美国证券交易委员会(以下简称“SEC”)披露如下信息:(1)在法案所规定的期间内该注册会计师事务所已为上市企业编制的审计报告;(2)在上市企业注册成立或以其他方式组织的外国司法管辖范围内,由政府实体持有的上市企业股份的百分比;(3)在与该注册会计师事务所相关的适用外国司法管辖的政府实体是否对上市企业拥有控股权;(4)、(5)则均为直接针对中国意识形态防范和国家安全泛化的条款。“CLOUD法案”<sup>[12]</sup>在第3节明确规定:“电子通信服务或远程计算服务的提供商应遵守本法案规定的义务,保存、备份或披露有线或电子通信的内容,以及在其拥有、保管或控制范围内与客户或订户有关的任何记录或其他信息,无论该通信、记录或其他信息是否存储于美国境内或境外”。“HFCAA法案”严重暴露了美国证券监管的政

治化<sup>[13]</sup>,严重破坏了证券行业的市场竞争机制,“CLOUD 法案”则确立了美国数据监管的“长臂管辖”机制。根据美国现行法案和政治风向,滴滴公司赴美上市必然存在数据泄露甚至被不法利用的风险。这一点体现于《网络安全审查办法》第十条国家安全风险因素中的第六项:“上市存在……大量个人信息被外国政府影响、控制、恶意利用的风险,以及网络信息安全风险”<sup>[14]</sup>。因此,数据跨境流动会对国家安全的维护提出全新的法治挑战,通过立法规制数据力量对维护国家安全至关重要,充分维护国家安全是数据跨境流动监管必须直面的问题。

## 1.2 个人数据保护层面的挑战

从滴滴公司存在的 16 项违法事实<sup>[13]</sup>可以看出,侵犯个人数据信息的情况有两种,其一是未经用户授权违法获取数据或超出用户授权过度收集数据,如违法获取或过度收集的用户个人信息数据;其二是背离数据授权使用范围处理数据,如在未明确告知乘客的情况下分析乘客的出行意图、常驻城市以及异地商务或异地旅游意向。无论是获取或收集用户的个人信息,还是处理用户的个人信息都需要用户的授权,且不能超出用户的授权范围,这是因为个人信息的收集、使用、共享以及加密保护都应在一定程度上获得受影响个人的知情通知和同意<sup>[15]</sup>,使他们有能力控制关涉自身的数据信息<sup>[16]</sup>。

美国近年来发生的多起案例也表明数据跨境流动会对个人数据保护提出法治挑战。例如,2017 年 5 月至 7 月,Equifax 发生数据泄露,并于当年 9 月 7 日披露了数据泄露的影响范围,包括 1.479 亿美国公民、1 520 万英国公民和约 19 000 名加拿大公民的个人数据信息被泄露,2019 年 7 月 22 日,Equifax 同意与联邦贸易委员会(FTC)、美国消费者金融保护局(CFPB)、美国 48 个州、华盛顿特区和波多黎各达成和解,协议总额达 7 亿美元<sup>[17]</sup>。又如,2019 年 7 月 29 日 Capital One 公开承认,一名黑客未经授权访问了美国和加拿大 1.06 亿人(美国公民约 1 亿人,加拿大公民约 600 万人)的账户和身份信息<sup>[18]</sup>,2022 年 2 月 7 日,美国联邦法院初步批准了 Capital One 数据泄露事件有关的集体诉讼和解,和解要求 Capital One 建立一个 1.9 亿美元的结算基金并提供其他救济服务<sup>[19]</sup>。此外,2021 年 8 月 16 日 T-Mobile 宣布,一名黑客非法访问了超过 7 600 万

美国公民的个人数据,并就此事件提起了多起数据泄露集体诉讼,2022 年 7 月 T-Mobile 在密苏里州联邦法院的听证会上同意就数据泄露和随后的集体诉讼达成 3.5 亿美元的和解<sup>[20]</sup>。在这三个案例中,企业的业务范围均覆盖全球多个国家,且前两个案例的数据泄露范围涉及多国公民。根据诉讼案由可知,这三家企业均因未能有效保护用户数据安全致使用户数据未经授权而被非法利用或处于被非法利用的危险之中,其中 Capital One 数据泄露案件的黑客佩奇·汤普森<sup>[21]</sup>还在 2019 年 4 月发布了如何获取公司凭证以提取更多数据的说明<sup>[22]</sup>。从上述案例不难发现,因数据传输技术等原因,跨境数据流动存在个人数据泄露的风险,如何保护个人数据安全,避免数据未经授权获取或使用是数据跨境流动监管必须直面的又一问题。

当然,在保护个人数据的同时也要注意统筹发展和安全。个人数据保护规则的制定和实施要同经济社会的发展相适应。对此,有研究根据数据产权配置对市场经济发展的影响得出结论:产权的最优配置关键取决于数据的价值,即取决于产生数据的市场和使用数据的市场之间的相对权重,当产生数据的市场权重更大时,应当尽可能保护个人的数据权利;当使用数据的市场权重更大时,应尽可能鼓励个人授权企业使用数据,促进社会经济的发展<sup>[23]</sup>。国内学者也指出:“要在个人信息保护与大数据发展之间实现平衡”<sup>[24]</sup>,并且“应在立法层面平衡数据交易与个人信息权利保护之间的关系”<sup>[25]</sup>。因此,如何在促进数字经济发展的同时保护个人数据安全是数据跨境流动在个人数据保护层面提出的全新法治挑战。

## 2 应对挑战的立法现状及实践难点

### 2.1 国家安全层面的立法现状及实践难点

我国现行法律法规对数据跨境流动在国家安全层面的应对主要体现在如下三个方面。

首先是坚持总体国家安全观。对此,党的二十大报告指出:“必须坚定不移贯彻总体国家安全观,把维护国家安全贯穿党和国家工作各方面全过程,确保国家安全和社会稳定”<sup>[2]</sup>,坚持总体国家安全观明确规定在《中华人民共和国数据安全法》(以下简称《数据安全法》)<sup>[26]</sup>第四条当中,并全面贯穿于我国现行法律法规的各项规定,其一,既重视数据

处理过程发生在境内的安全,又重视数据跨境流动及在境外开展数据处理活动的安全,这明确体现在《数据安全法》第二条的规定当中;其二,既重视数字经济的发展问题,又重视数据处理和流动过程的国家安全问题,发展和安全是数字经济的两件大事,充分发挥海量数据和丰富应用场景优势,这明确体现在《数据安全法》第二章的规定当中;其三,既重视自身安全,又重视共同安全,打造网络空间命运共同体,推动各方朝着互利互惠、共同安全的目标相向而行,这明确体现在《数据安全法》第二十六条和第三十六条的规定当中。

其次是建立数据分类分级保护制度,加强对重要数据的保护。由于数据具有非排他性<sup>[5]</sup>,这意味着数据的传输是几乎没有成本和损耗的,那些“一旦遭到篡改、破坏、泄露或者非法获取、非法利用等,可能危害国家安全、经济运行、社会稳定、公共健康和安全等”<sup>[27]</sup>的重要数据必须要通过一定的技术手段限制跨境流动。通过构建重要数据评估标准,建立数据分类分级保护制度,从而加强对重要数据的保护。这明确体现在《数据安全法》第二十一条的规定当中。在具体实践中,我国工业和信息化部发布的《工业和信息化领域数据安全管理办法(试行)》公开征求意见稿中第二章<sup>[28]</sup>明确规定了工业和信息化领域数据的分类分级管理,其他各部委及省份也在根据实际情况确定重要数据的具体目录。

最后是明确数据安全保护义务和法律责任。《数据安全法》在第四章规定了数据安全保护义务,在第五章规定了违反义务需承担的法律后果,其中第三十一条明确规定了重要数据的出境安全管理,第四十六条则明确规定了违反第三十一条规定,向境外提供重要数据的法律责任。结合上述条文与滴滴公司及该企业直接负责的主管人员的行政处罚情况<sup>[4]</sup>来看,滴滴公司很可能涉嫌违反《数据安全法》第三十一条规定,将该企业在我国境内运营中收集和产生的重要数据输出境外。除了《数据安全法》以外,《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)第四十条至第四十二条也在国家安全层面对个人信息跨境流动的监管做了具体规定<sup>[29]</sup>。

综合上述,重要数据目录管理具有动态属性,

该属性引发的时效难题是监管数据跨境流动以维护国家安全的实践难点。从滴滴公司违法获取或过度收集的数据信息种类不难看出,这些数据信息的种类与软硬件功能和数字技术的发展密切关联。随着软硬件功能越来越丰富,数据挖掘和分析技术越来越先进,数据的更新速度会不断加快,数据规模会越来越庞大,数据种类划分也会越来越精细,数据目录的变化周期就会越来越短,重要数据的目录管理也就越来越呈现出动态属性,这一动态属性在《工业和信息化领域数据安全管理办法(试行)》公开征求意见稿第七条<sup>[28]</sup>就有明确的体现。重要数据目录列选的动态属性意味着重要数据的评估标准和保护力度也要紧跟时代的发展,在这一情形下如何保证重要数据目录列选的时效性是实践过程中的具体困难。完善立法以解决这一实践难点,是应对数据跨境流动提出的国家安全挑战的有效途径。

## 2.2 个人数据保护层面的立法现状及实践难点

我国现行法律法规对数据跨境流动在个人数据保护层面挑战的应对主要体现在如下四个方面。

首先是明确个人数据及相关概念的定义。由于数据是记录事实信息的一种特殊表达方式,是“信息”这一概念的一部分<sup>[30]</sup>,因此个人数据亦可被解释为个人信息的一部分。个人信息的定义见于《个人信息保护法》第四条第一款规定:“个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息,不包括匿名化处理后的信息”<sup>[29]</sup>;数据的定义则见于《数据安全法》第三条规定:“本法所称数据,是指任何以电子或者其他方式对信息的记录”<sup>[27]</sup>。结合这两部法律可知,个人数据是指任何以电子或者其他方式对个人信息的记录,属于受我国法律法规保护的个人信息范畴。

其次是突出对敏感个人数据信息的保护。《个人信息保护法》第二十八条第一款定义了敏感个人信息,是指“一旦泄露或者非法使用,容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息,包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息,以及不满十四周岁未成年人的个人信息”<sup>[29]</sup>。根据该条规定,记录敏感信息的个人数据也应当被特殊保护,在滴滴公司存在的16项违法事实<sup>[3]</sup>当中,违法获

取用户的人脸识别信息就属于敏感个人信息之一。

再次是规定了处理个人信息的情形、基本原则、具体规则以及对个人数据信息跨境流动监管的规则。处理个人信息的情形具体规定在《个人信息保护法》第四条第二款,即“只有在具有特定的目的和充分的必要性,并采取严格保护措施的情形”,处理敏感个人信息的情形则规定在第二十八条第二款。处理个人数据信息包括规定在《个人信息保护法》的七大基本原则,其一是第五条规定的“合法、正当、必要、诚信”原则,其二和其三是第六条第一款和第二款规定的“目的明确合理且直接相关”和“最小范围”原则,其四是第七条规定的“公开透明”原则,其五是第八条规定的“准确完整”原则,其六、其七是第九条规定的“责任负担”原则和“数据安全”原则。个人数据信息处理的具体规则包括规定在《个人信息保护法》第十三条的前提条件、第十四条和第十五条规定的“个人同意”的具体要求、第十七条规定的“真实、准确、完整”的告知要求以及第十八条规定的“不告知”情形,第二十九条至第三十二条则规定了敏感个人信息处理的具体规则。对个人数据信息跨境流动监管的规则,则包括《个人信息保护法》第三十八条规定的前提条件和第三十九条规定的“告知—同意”规则<sup>[29]</sup>。

最后还规定了个人在个人信息处理活动中的权利、个人信息处理者的义务、履行个人信息保护职责的部门以及违法行为需承担的法律后果。例如《个人信息保护法》第六十六条明确规定“对违法处理个人信息的应用程序,责令暂停或者终止提供服务”<sup>[29]</sup>,对应了网络安全审查办公室对“滴滴出行”2021年7月2日启动网络安全审查<sup>[31]</sup>,并于7月4日下架“滴滴出行”App<sup>[32]</sup>,7月9日下架“滴滴企业版”等25款App<sup>[33]</sup>的法律依据。

综上所述,个人对其个人数据信息的处理可以设定一定授权处理范围,这明确规定在《个人信息保护法》第四十四条:“个人对其个人信息的处理享有知情权、决定权,有权限制或者拒绝他人对其个人信息进行处理;法律、行政法规另有规定的除外”<sup>[29]</sup>。又如 Facebook 早在 2015 年就发现了剑桥分析公司滥用其用户信息的行为,亦即 Facebook 明知滥用其用户信息的行为是超出用户授权范围的,但两年多来一直没有采取有效措施纠正<sup>[34]</sup>。《个人信息保护

法》第六条第二款明确规定了收集个人数据信息“应当限于实现处理目的的最小范围”<sup>[29]</sup>,这不仅对个人数据的收集范围做了限定,还意味着处理数据的范围应当与既定目的的实现相吻合。由于数字经济发展迅速,收集数据时的目的与收集完成准备处理数据时的目的可能会在合理范围内有所变化,如何根据客观经济规律认定这一合理范围,从而协调个人数据保护与经济发展的关系是实践过程中的具体困难。

### 3 突破实践难点的现实路径

#### 3.1 以区块链技术赋能重要数据目录的动态管理

重要数据目录管理的动态属性引发的时效难题,是监管数据跨境流动以维护国家安全的实践难点。随着数字政府建设的稳步推进,数字技术已经逐步融入到政府管理与服务的方方面面,在实践中,英国、法国、俄罗斯、瑞士、瑞典、芬兰、爱沙尼亚等国政府已经在公共服务领域广泛采用了区块链技术<sup>[35]</sup>。而针对数据目录的动态管理方面,现在已经有“目录区块链”系统应用于数字政府建设的实例。北京市人民政府在 2019 年深入实施北京大数据行动计划,打造了“目录区块链”<sup>[36]</sup>系统,该系统秉持职责为根、目录为干、数据为叶的三级目录体系建设路径,将全市政府部门、区的职责、目录和系统“上链”锁定,完成“上户口”,实现数据和职责的强关联、数据变化的实时探知以及数据访问的全程留痕,有效解决了大数据工作中长期存在的共享难、协同散、应用弱等问题。如果能将北京市“目录区块链”系统建设的经验应用于重要数据目录列选,建设以硬软件功能为纲、职责为根的目录体系,从而实现对数据变化的实时探知,可以有效解决重要数据目录列选的动态属性引发的时效难题。

所谓以硬软件功能为纲,是由于数据的产生大多与硬软件功能相关联,2021 年 9 月 1 日,五部门联合约谈了 11 家网约车平台公司,约谈要求“各平台公司要检视自身存在的问题,立即整改不合规行为……各平台公司在用户数据收集、传输、存储、处理等环节,要依法建立相关数据安全管理制度,采取必要的安全技术和管理措施”<sup>[37]</sup>。据此,不合规行为可能并非只存在于滴滴公司一家,企业获取因硬件功能产生的数据信息也是通过设计平台 App 的软件功能运行机制来实现的。因此,要想有效探知

重要数据的实时变化情况,就必须以硬软件功能为纲,对因硬软件功能产生的数据进行类别划分,并在此基础上评估这些数据对于维护国家的价值,依据评估结论建立重要数据目录,并即时关注硬软件功能的更新情况,以便实时更新重要数据目录。

所谓以职责为根,是要求各部门、各行业、各地区明确自身在数据识别、分类分级中的工作职责。根据行业要求、特点、业务需求、数据来源和用途等因素,来对识别数据进行分类。并根据数据遭到篡改、破坏、泄露或者非法获取、非法利用,对国家安全、公共利益或者个人、组织合法权益等造成的危害程度,来对数据进行分级。最后,利用区块链的透明、可回溯、不可篡改等特性<sup>[38]</sup>,实现重要数据变化的实时探知和重要数据目录的动态管理,从而有效解决时效性难题。

在具体应用方面,一项研究<sup>[39]</sup>表明,区块链技术可以有效解决与现有信息收集和共享系统相关的信息安全和效率问题。该研究运用区块链技术构建了一个信息收集和共享模型,可以在保证系统安全和用户隐私的前提下实时探知并共享患者的医疗记录。换言之,区块链技术既可以提供安全的信息系统,同时也增加了患者共享医疗记录的动机,并且通过开发 Android 软件应用程序来实现可行性。另一项研究<sup>[40]</sup>也是以医疗数据的收集和共享为视角,证明了通过采用区块链可以保证医疗数据的正确性和患者的隐私,特定数据的完整性也可以通过区块链技术的智能合约控制来实现。此外,还有一些研究<sup>[41-42]</sup>也表明区块链技术在数据收集和共享方面兼具安全性和效率,证实了其应用于重要数据目录动态管理的可行性。

因此,相关部门可以通过区块链技术开发软件程序实时检测重要数据情况,构建以软件功能为纲、职责为根的重要数据目录动态管理系统,解决国家数据安全层面的管理时效难题。并在此基础上建立数据安全监测预警与应急管理机制,从而有效应对数据跨境流动在国家安全维护层面提出的法治挑战。

### 3.2 以区块链技术协调个人数据保护和经济发展

如何确定个人数据利用的底线,划定处理数据的合理范围,从而协调个人数据保护与经济发展的

关系,是监管数据跨境流动以保护个人数据的实践难点。对此,有学者认为:“数字社会中作为权利客体的个人信息具有固有的人格与天然的财产双重价值……个人信息权的人格权属性具有对数据财产权的优位性,它因此是信息处理的底线”<sup>[43]</sup>,他还基于个人数据主体与数据处理器之间的实质不平等关系指出,可以借由“告知—选择”的行权方式达到弱化权利移转效果的目的,既可以保护处于弱势的个人数据主体,也可以降低交易磋商的难度,从而促进数据流通,进而推动经济发展<sup>[44]</sup>。不难发现,所谓“告知—选择”说主要针对数据处理器与个人数据主体之间“一对多式”的格式合同情形,这一情形下个人数据主体显然居于弱势,而《中华人民共和国民法典》(以下简称《民法典》)第四百九十六条至第四百九十八条<sup>[45]</sup>已经对格式条款加以规定,综合《个人信息保护法》规定的个人数据信息处理的“告知—同意”模式和《民法典》格式条款的规定可以为解决这一问题提供一条救济路径,但该路径相对比较滞后,亟需一条更为及时的保护途径。

引入区块链技术来平衡个人数据主体与数据处理器之间的实质不平等关系,相对于传统救济途径,保护更为及时。《个人信息保护法》第四条规定将匿名化处理后的信息排除在了个人信息之外,“匿名化”是指“个人信息经过处理无法识别特定自然人且不能复原的过程”<sup>[29]</sup>,从这一规定不难发现,企业如果将个人数据信息匿名化处理之后,在无涉国家安全、公共安全等的前提下,可以自由地进行数据跨境流动。这是由于匿名化处理之后,个人数据的人格权属性得到了最大程度的保护。然而,现实当中很难做到完全匿名化,且完全匿名化处理之后数据的经济价值也可能会有所降低。如果可以将格式合同关涉个人数据中人格权益的条款由国家监督制定,且可以为行业通用,不能篡改,那么就可以平衡个人数据主体与数据处理器之间的实质不平等关系。而实现这一情形的技术手段,就是以太坊区块链技术。

以太坊区块链技术中的智能合约可以将合同内容用编程的方式写入区块链网络当中,一旦合同被写入,其内容将不可更改,合同双方必须按约执行<sup>[46]</sup>。目前已有研究<sup>[47]</sup>引入智能合约技术以实现基于区块链的激励兼容机制,兼顾效率的提升和用户

信息安全的需求。国家可以通过立法将保护个人数据中人格权益的条款规范化,并写入以太坊区块链技术支持的智能合约当中,从而有效杜绝企业滥用个人数据侵害人格权益的行为。这项技术已经被应用到患者医疗数据保护方面,通过执行基于区块链的智能合约来设计安全保护协议,兼顾经济效益和信息安全<sup>[48]</sup>。

综上所述,个人数据利用的底线是不能侵犯个人数据主体的人格尊严,结合以太坊区块链技术将人格权益保护条款写入智能合约,可以有效平衡个人数据主体与数据处理者的市场地位,个人数据财产权益的实现则由市场规律决定,这也契合了党的二十大报告中“充分发挥市场在资源配置中的决定性作用,更好发挥政府作用”<sup>[2]</sup>的论述。

#### 4 结论

在数字经济快速发展且覆盖全球的今天,数据跨境流动已成为我国必须直面的问题。数据跨境流动监管面临两大法治实践困难,即重要数据目录的动态管理和个人数据保护与经济协调平衡。针对这两大难题,现行立法和相关理论提出了一定的解决途径,然而这些解决途径相对比较滞后,难以应对快速发展的数字经济现实。区块链技术有效弥补了这一局限,用技术监管技术的法治思维,可以适应数字经济快速发展的实际情况,从而有效应对数据跨境流动提出的法治挑战。

#### 参考文献

- [1] 习近平.不断做强做优做大我国数字经济[J].中国信息安全,2022(1):16-20.
- [2] 习近平.高举中国特色社会主义伟大旗帜 为全面建设社会主义现代化国家而团结奋斗[N].人民日报,2022-10-26(001).
- [3] 国家互联网信息办公室有关负责人就对滴滴全球股份有限公司依法作出网络安全审查相关行政处罚的决定答记者问[EB/OL].[2022-11-02].http://www.cac.gov.cn/2022-07/21/c\_1660021534364976.htm.
- [4] 国家互联网信息办公室对滴滴全球股份有限公司依法作出网络安全审查相关行政处罚的决定[EB/OL].[2022-11-02].http://www.cac.gov.cn/2022-07/21/c\_1660021534306352.htm.
- [5] SLAUGHTER M J, MCCORMICK D H. Data is power[J]. Foreign Affairs, 2021, 100(3): 54-62.
- [6] KERASOVITIS K. The data gaze: capitalism, power and perception, information[J]. Communication & Society, 2019, 122(13): 2033-2036.
- [7] 陈鹏.数据的权力:应用与规制[J].安徽师范大学学报(人文社会科学版),2021,49(5):111-119.
- [8] RAZALI N A M, MALIZAN N A, HASBULLAH N A, et al. Opinion mining for national security: techniques, domain applications, challenges and research opportunities[J]. Journal of Big Data, 2021, 8(1): 150.
- [9] How the Facebook-Cambridge Analytica saga unfolded[EB/OL].[2022-11-02].https://www.bloomberg.com/news/articles/2018-03-21/understanding-the-facebook-cambridge-analytica-story-quicktake?lead\_source=uverify%20wall.
- [10] HOWARD P N. Our data, ourselves[J]. Foreign Affairs, 2018, 229: 27-28.
- [11] Congress of the United States. Holding foreign company accountable act[L]. (2020-12-02).https://www.congress.gov/116/plaws/publ222/PLAW-116publ222.pdf.
- [12] Congress of the United States. Clarifying lawful overseas use of data act[L]. (2020-03-xx).https://www.congress.gov/115/bills/hr4943/BILLS-115hr4943ih.pdf.
- [13] 马更新,郑英龙,程乐.《外国公司问责法案》的美式“安全观”及中国应对方案[J].商业经济与管理,2020(9):82-91.
- [14] 国家互联网信息办公室,国家发展和改革委员会,工业和信息化部,公安部,国家安全部,财政部,商务部,中国人民银行,国家市场监督管理总局,国家广播电视总局,中国证券监督管理委员会,国家保密局,国家密码管理局.网络安全审查办法[L]. 2021-12-28.
- [15] MCLAUGHLIN P. Cross-border data flows and increased enforcement[J]. IEEE Security & Privacy, 2008, 6(5): 58-61.
- [16] HARPER Jim. Understanding privacy and the real threats to it[J]. Policy Analysis, 2004, 520: 1-17.
- [17] Case 1:19-cv-03297-TWT[EB/OL].[2022-11-02].https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3203-equifax-inc.
- [18] Information on the Capital One cyber incident[EB/OL].[2022-11-02].https://www.capitalone.com/digital/facts2019/.
- [19] Case 1:19-cv-02969-AJT-JFA[EB/OL].[2022-

- 11-02].<https://www.capitalonesettlement.com/Content/Documents/Final%20Approval%20Order.pdf>.
- [20] Case 4:21-md-03019[EB/OL].[2022-11-02].[https://www.pacermonitor.com/public/case/42873727/In\\_re\\_TMobile\\_Customer\\_Data\\_Security\\_Breach\\_Litigation](https://www.pacermonitor.com/public/case/42873727/In_re_TMobile_Customer_Data_Security_Breach_Litigation).
- [21] GANDEL S.What we know so far about accused Capital One hacker paige thompson[EB/OL].[2022-11-02].<https://www.cbsnews.com/news/paige-thompson-what-we-know-about-accused-capital-one-breach-hacker-2019-07-31/>.
- [22] Case 1:19-cv-00979[EB/OL].[2022-11-02].<https://s3.documentcloud.org/documents/6226401/Capital-One-Data-Breach-Stamped-Complaint.pdf>.
- [23] DOSIS A, SAND-ZANTMAN W.The ownership of data[J].Journal of Law Economics & Organization, Oxford University Press, 2022. DOI: 10.1093/jleo/ewac001.
- [24] 周汉华.探索激励相容的个人数据治理之道——中国个人信息保护法的立法方向[J].法学研究, 2018, 40(2): 3-23.
- [25] 苗泽一.数据交易市场构建背景下的个人信息保护研究[J/OL].政法论坛: 1-11[2022-11-21].<http://kns.cnki.net/kcms/detail/11.5608.D.20221107.1113.004.html>.
- [26] 全国人民代表大会常务委员会.中华人民共和国数据安全法[L].2021-06-10.
- [27] 国家互联网信息办公室.数据出境安全评估办法[L].2022-07-07.
- [28] 中华人民共和国工业和信息化部.《工业和信息化领域数据安全管理办法(试行)》公开征求意见稿[L].2022-02-10.[https://www.miit.gov.cn/api-gateway/jpaas-web-server/front/document/file-download?fileUrl=/cms\\_files/filemanager/1226211233/attach/202112/4ca-3dd7c3acd48c0b4ab490dcbc31cbb.pdf&fileName=附件1-《工业和信息化领域数据安全管理办法\(试行\)》公开征求意见稿.pdf](https://www.miit.gov.cn/api-gateway/jpaas-web-server/front/document/file-download?fileUrl=/cms_files/filemanager/1226211233/attach/202112/4ca-3dd7c3acd48c0b4ab490dcbc31cbb.pdf&fileName=附件1-《工业和信息化领域数据安全管理办法(试行)》公开征求意见稿.pdf).
- [29] 全国人民代表大会常务委员会.中华人民共和国个人信息保护法[L].2021-08-20.
- [30] JONES C I, TONETTI C.Nonrivalry and the economics of data[J].American Economic Review, 2020, 110(9): 2819-2858.
- [31] 网络安全审查办公室关于对“滴滴出行”启动网络安全审查的公告[EB/OL].[2022-11-02].[http://www.cac.gov.cn/2021-07/02/c\\_1626811521011934.htm](http://www.cac.gov.cn/2021-07/02/c_1626811521011934.htm).
- [32] 关于下架“滴滴出行”App的通报[EB/OL].[2022-11-02].[http://www.cac.gov.cn/2021-07/04/c\\_162-7016782176163.htm](http://www.cac.gov.cn/2021-07/04/c_162-7016782176163.htm).
- [33] 关于下架“滴滴企业版”等25款App的通报[EB/OL].[2022-11-02].[http://www.cac.gov.cn/2021-07/09/c\\_1627415870012872.htm](http://www.cac.gov.cn/2021-07/09/c_1627415870012872.htm).
- [34] Case 3:19-cv-04241[EB/OL].[2022-11-02].<https://www.sec.gov/litigation/complaints/2019/comp-pr2019-140.pdf>.
- [35] 何翔舟.基于区块链赋能的政府治理成本研究[M].北京:人民出版社, 2021.
- [36] 陈吉宁.政府工作报告[N].北京日报, 2020-01-19(001).
- [37] 五部门联合约谈11家网约车平台公司[EB/OL].[2022-11-02].<https://mp.weixin.qq.com/s/VDvz1-K18Go73o-fD6tLIQQ>.
- [38] 张鹏.区块链赋能下的数字法治政府建设:内涵、关联及路径[J].电子政务, 2022(7): 88-97.
- [39] SADEGHI J K, PRYBUTOK V R, SAUSER B, et al.Theoretical and practical applications of blockchain in healthcare information management[J].Information & Management, 2022, 59(6).
- [40] LEE J S, CHEW C J, LIU J Y, et al.Medical block-chain: data sharing and privacy preserving of EHR based on smart contract[J].Journal of Information Security and Applications, 2022, 65.
- [41] TOUFAILY E, ZALAN T, DHAOU S B.A framework of blockchain technology adoption: an investigation of challenges and expected value[J].Information & Management, 2022, 58(3).
- [42] CASADO-VARA R, CHAMOSO P, PRIETO F D L, et al.Non-linear adaptive closed-loop control system for improved efficiency in IoT-blockchain management[J].Information Fusion, 2019(49): 227-239.
- [43] 彭诚信.论个人信息的双重法律属性[J].清华法学, 2021, 15(6): 78-97.
- [44] 彭诚信, 史晓宇.个人信息财产价值外化路径新解——基于公开权路径的批判与超越[J].华东政法大学学报, 2022, 25(4): 41-57.
- [45] 全国人民代表大会.中华人民共和国民法典[L].2020-05-28.
- [46] 傅丽玉, 陆歌皓, 吴义明, 等.区块链技术的研究及其发展综述[J].计算机科学, 2022, 49(S1): 447-

461, 666.

- [47] ALREBDI N, ALABDULATIF A, IWENDI C, et al. SVBE: searchable and verifiable blockchain-based electronic medical records system[J]. Scientific Reports, 2022; 1-11. DOI: 10.1038/s41598-021-04124-8.
- [48] ZHANG G, YANG Z, LIU W. Blockchain-based privacy preserving e-health system for healthcare data

in cloud[J]. Computer Networks, 2022, 203. DOI: 10.1016/j.comnet.2021.108586.

(收稿日期: 2022-11-21)

作者简介:

杜昕(1998-), 男, 硕士研究生, 主要研究方向: 数字法治政府建设、数据跨境流动监管。

(上接第 36 页)

faces attributes(celeba) dataset[J]. Retrieved August, 2018, 15(2018): 11.

- [15] 刘春泉. 换脸软件涉嫌公众安全 人体生物识别信息管理要跟上[N]. 第一财经日报, 2019-09-24(A11).
- [16] 方艳梅. 深度伪造对人脸识别支付系统安全性的挑战与应对[J]. 金融科技时代, 2020, 28(3): 13-17.
- [17] 张怡铭. 虚假“刷脸”验证行为的刑法规制[J]. 中国

检察官, 2021(24): 30-34.

(收稿日期: 2022-12-30)

作者简介:

马梓为(2001-), 通信作者, 男, 本科, 主要研究方向: 网络空间安全。E-mail: 758093044@qq.com。

杨子琪(2002-), 男, 本科, 主要研究方向: 软件工程。

李晨帆(2002-), 男, 本科, 主要研究方向: 软件工程。

(上接第 44 页)

implemented in laws outside Europe[R]. 2018-01-08.

- [34] GREENLEAF G. It's nearly 2020, so what fate awaits the 1980 OECD privacy guidelines?(A background paper for the 2019 OECD privacy guidelines review)[R]. 2019-06-17.
- [35] 于柏华. 比例原则的权利内置论[J]. 法商研究, 2020, 37(4): 88-100.

- [36] 新华网. 习近平在中华人民共和国恢复联合国合法席位 50 周年纪念会议上的讲话(全文)[EB/OL]. (2021-10-25)[2022-11-12]. <https://baijiahao.baidu.com/s?id=1714558957877058899&wfr=spider&for=pc>.

(收稿日期: 2022-11-12)

作者简介:

张濛之(1999-), 女, 硕士研究生, 主要研究方向: 国际投资法、数据法、国际私法。



# 版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部

www.pcachina.cn